Lecture 4.

Def. A ring R is called commutative if

$ab = ba \quad \forall a, b \in R$.

Let R be a ring with $\mathbb{1}$.

Def. An element $a \in R$ is called invertible if there exists an element $b \in R$ such that $ab = ba = \mathbb{1}$.

Exercise. Such an element b is unique.

The element b is called the inverse of

a.

Notation: $b = a^{-1}$.

Exercise. $(a^{-1})^{-1} = a$.

Exercise. An element $a \in \mathbb{Z}(n)$ is invertible if and only if $\gcd(a, n) = 1$.

Invertible elements in $\mathbb{Z}/(8)$:

$1, 3, 5, 7.$

<u>Definition</u>. Let R be a commutative ring with $\mathbb{1}$. We say that R is a <u>field</u> if every nonzero element of R is invertible.

<u>Examples of Fields</u>: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; $\mathbb{Z}/(p)$, where p is a prime number.

<u>Lemma</u>. Let R be a field. If $0 \neq a \in R$, $0 \neq b \in R$ then $0 \neq ab$.

<u>Proof</u>. Since $0 \neq a$ there exists an element $a^{-1} \in R$ such that $a^{-1} \cdot a = \mathbb{1}$. If $ab = 0$ then $a^{-1}(ab) = \mathbb{1} \cdot b = b = 0$, a contradiction. $\downarrow$

<u>Remark</u>. A ring where a product of two nonzero elements is $\neq 0$ is called a <u>domain</u>.

We proved that a field is a domain.

Characteristic of a field.

Let R be a field and let $\mathbb{1}$ be the identity element of R. There are two possibilities:

1) For an arbitrary nonzero integer n we have $n\mathbb{1} \neq 0$.

If $n \geq 1$ then $n\mathbb{1} = \underbrace{\mathbb{1} + \mathbb{1} + \dots + \mathbb{1}}_{n}$.

If $n \leq -1$, say, $n = -5$ then

$(-5)\mathbb{1} = -(\underbrace{\mathbb{1} + \mathbb{1} + \dots + \mathbb{1}}_{5})$.

2) There exists a nonzero integer n such that $n\mathbb{1} = 0$.

Let's analyse the 1st possibility.

We claim that in this case for an arbitrary nonzero integer n and an arbitrary nonzero element $a \in R$

$$n a \neq 0.$$

Indeed, let $na = 0$. Without loss of generality we may assume that $n \geq 1$. Indeed, if $(-5)a = -(5a) = 0$ then $5a = 0$.

But $na = \underbrace{a + a + \cdots + a}_{n} = (\underbrace{1 + 1 + \cdots + 1}_{n}) a =$

$= (n 1) a.$

Since R is a domain $na = 0$ implies

$n 1 = 0$ or $a = 0$, a contradiction.

If the 1st possibility holds, then we say that the field R <u>has zero characteristic</u>, $\operatorname{char} R = 0$.

<u>Examples:</u> $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Now let us discuss the Possibility 2:

there exists a nonzero integer n such that $n\mathbb{1}=0$.

Again without loss of generality we assume that $n \geq 1$.

The set $S=\{k\geq 1 \mid k\mathbb{1}=0\}$ is not empty.

For example, $n \in S$.

<u>Basic Principle</u>: every nonempty set of positive integers contains a minimal element.

Let p be a minimal element of the set S.

<u>Claim</u>: p is a prime number.

Indeed, let $p = p_1 \cdot p_2$, where p_1, p_2 are positive integers; $p_1 > 1$, $p_2 > 1$, which implies that both p_1 and p_2 are $< p$.

We have $(\underbrace{\mathbb{1} + \dots + \mathbb{1}}_{p_1})(\underbrace{\mathbb{1} + \dots + \mathbb{1}}_{p_2}) = \underbrace{\mathbb{1} + \dots + \mathbb{1}}_{p} = 0.$

Hence $p_1 \mathbb{1} = 0$ or $p_2 \mathbb{1} = 0$. In other words $p_1 \in S$ or $p_2 \in S$. But both p_1 and p_2 are $< p$, a contradiction.

<u>Def</u>. The prime number p is called the <u>characteristic</u> of the field R,

$$p = \operatorname{char} R.$$

For an arbitrary element $a \in R$

$pa = (p\mathbb{1})a = 0.$

<u>Example.</u> $\operatorname{char} \mathbb{Z}(p) = p$.

Polynomials. ~~and Rational functions~~

Let F be a field. A polynomial over F is a formal expression

$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n,$$

where $n \geq 1$; $a_0, a_1, \dots, a_n \in F$. We assume that $a_n \neq 0$, otherwise we just don't mention this summond. Then

$$\deg f(t) = n.$$

The coefficient a_0 is called the <u>constant term</u> of the polynomial $f(t)$.

The coefficient a_n is called the <u>leading coefficient</u> of $f(t)$

Polynomials may be added and multiplied:

let $f(t) = a_0 + a_1 t + \cdots + a_n t^n$, $g(t) = b_0 + b_1 t + \cdots + b_m t^m$, $m \leq n$.

Then $f(t) + g(t) = (a_0 + b_0) + (a_1 + b_1) t + \cdots + (a_m + b_m) t^m + a_{m+1} t^{m+1} + \cdots + a_n t^n$;

$f(t)\, g(t) = a_0 b_0 + (a_1 b_0 + a_0 b_1) t + \cdots\ a_n b_m t^{n+m}$,

we just expand brackets.

With these addition & multiplication the set of polynomials

$$F[t]$$

becomes a ring.

This ring is a domain, but not a field.

Division of polynomials.

Theorem. Given two polynomials $f(t)$ and $g(t) \neq 0$, $g(t)$ is not a constant, there exist unique polynomials $q(t)$ and $r(t)$ such that

$$f(t) = g(t)\, q(t) + r(t), \quad \deg r(t) < \deg g(t).$$

Proof. Induction on $\deg f(t)$. Let $\deg f(t) = 0$, i.e. $f(t)$ is a constant. By the assumption of the theorem $\deg g(t) \geq 1$. We have

$$f(t) = g(t) \cdot 0 + f(t), \quad \deg f(t) < \deg g(t).$$

Now let $\deg f(t) > 0$. If $\deg f(t) < \deg g(t)$, then we can still choose the presentation

$$f(t) = g(t) \cdot 0 + f(t).$$

Suppose that $\deg f(t) \geq \deg g(t)$.

Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n$, $a_n \neq 0$,

$g(t) = b_0 + b_1 t + \cdots + b_m t^m$, $b_m \neq 0$, $m \leq n$.

The polynomial

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t)$$

has degree $< n$ because ~~so~~ the coefficients at t^n cancel.

By the induction assumption there exist polynomials $q_1(t)$, $r_1(t)$, $\deg r_1(t) < \deg g(t)$, such that

$$f_1(t) = g(t)\, q_1(t) + r_1(t).$$

Now $f(t) = f_1(t) + \frac{a_n}{b_m} t^{n-m} g(t) =$

$= g(t)\, q_1(t) + r_1(t) + \frac{a_n}{b_m} t^{n-m} g(t) \quad =$

$$g(t)\left(q_1(t)+\frac{a_n}{b_m}t^{n-m}\right)+r_1(t).$$

It remains to let $q(t)=q_1(t)+\frac{a_n}{b_m}t^{n-m}$,

$r(t)=r_1(t)$.

Now let us prove uniqueness of $q(t), r(t)$.

Let $f(t)=g(t)q(t)+r(t)=g(t)\tilde{q}(t)+\tilde{r}(t)$,

$\deg r(t), \deg\tilde{r}(t)<\deg g(t)$.

We have

$$g(t)\left(q(t)-\tilde{q}(t)\right)=\tilde{r}(t)-r(t).$$

the polynomial $\tilde{r}(t)-r(t)$ of degree $<g(t)$ can not be divisible by $g(t)$ unless $\tilde{r}(t)-r(t)=0$.

Once we established that $r(t)=\tilde{r}(t)$ it follows that

$$g(t)\,q(t) = g(t)\,\tilde{q}(t)$$

and therefore $q(t) = \tilde{q}(t)$. $\downarrow$

<u>Def.</u> An element $\alpha \in F$ of the field F is called a <u>root</u> of a polynomial $f(t)$ if $f(\alpha) = 0$.

<u>Theorem.</u> An element $\alpha \in F$ is a root of a polynomial $f(t)$ if and only if $f(t)$ is divisibly by $t - \alpha$.

Proof. If $f(t) = (t-\alpha) f_1(t)$ then

$$f(\alpha) = (\alpha - \alpha)\, f_1(\alpha) = 0.$$

Suppose that $f(\alpha) = 0$. Let's divide $f(t)$ by $t - \alpha$ with a remainder:

$$f(t) = (t - \alpha)\, q(t) + r(t).$$

Since $\deg r(t) < \deg(t-\alpha) = 1$ it follows that $\deg r(t) = 0$, hence $r(t)$ is a constant, $r(t) = \beta \in F$. We have

$$f(t) = (t-\alpha)\, q(t) + \beta .$$

Substitute $t = \alpha$.

$0 = f(\alpha) = (\alpha - \alpha)\, q(\alpha) + \beta$, hence $\beta = 0$.

We proved that $f(t)$ is divisible by $t-\alpha$. I

<u>Theorem</u>. A nonzero, polynomial of degree n can not have more than n distinct roots.

<u>Proof</u>. Suppose that $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ are roots of a polynomial $f(t)$, $\deg f(t) = n$.

By the Theorem above

$$f(t) = (t - \alpha_1)\, f_1(t).$$

Substitute $t = \alpha_2$.

$$0 = f(\alpha_2) = (\alpha_2 - \alpha_1)\, f_1(\alpha_2).$$

Since $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ are distinct we have $\alpha_2 - \alpha_1 \neq 0$. Therefore $f_1(\alpha_2) = 0$.

Again by the theorem above

$$f_1(t) = (t - \alpha_2)\, f_2(t),$$

and

$$f(t) = (t - \alpha_1)(t - \alpha_2)\, f_2(t).$$

Substitute $t = \alpha_3$.

$$0 = f(\alpha_3) = \underbrace{(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)}_{\neq 0}\, f_2(\alpha_3),$$

$$f_2(\alpha_3) = 0, \quad f_2(t) = (t - \alpha_3)\, f_3(t)$$

and so on.

At the $(n+1)$-th step we get

$$f(t) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_{n+1})\, f_{n+1}(t).$$

But the degree of the right hand side is $\geq n+1$, a contradiction. $\bar{\downarrow}$

For an arbitrary polynomial $f(t)$ the set $f(t)F[t]$ of all multiples of $f(t)$ is an ideal of $F[t]$. We denote this ideal as: $(f(t))$.

~~Theorem. An arbitra~~

Example. $F = \mathbb{Z}(5)$. Divide x^3+1 by x^2+1 with a remainder.

$$x^3+1 = x(x^2+1) - x + 1, \quad \deg(-x+1) < \deg(x^2+1)$$

We are done.